UNITED STATES PATENT AND TRADEMARK OFFICE

MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/666,207	09/18/2003	Laurent Eschenauer	MR2833-34	8288

4586 7590 06/21/2007

ROSENBERG, KLEIN & LEE
3458 ELLICOTT CENTER DRIVE-SUITE 101
ELLICOTT CITY, MD 21043

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
06/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/666,207	Applicant(s) ESCHENAUER ET AL.	
	Examiner Nirav Patel	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 March 2007 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) ______ is/are withdrawn from consideration.

5)□ Claim(s) ______ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)□ Claim(s) ______ is/are objected to.

8)□ Claim(s) ______ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on ______ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. ______.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date ______.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ______ .
5) □ Notice of Informal Patent Application
6) □ Other: ______.

DETAILED ACTION

1. Applicant's amendment filed on March 29, 2007 has been entered. Claims 1-22 are pending. Claims 1, 16 and 22 are also amended by the applicant.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Greenfield (US Patent No 6,748,528) in view of Garay et al (US Patent No. 6,839,436) and in view of Wong (US Pub. No. 2002/0146127).

As per claim 1, Greenfield teaches:

prior to deployment, storing, in each node, a respective key ring [Fig. 3], said key rings of at least pair of said sensor nodes having a common key [col. 9 lines 58-61]. Greenfield teaches key ring including a plurality of keys [col. 3 lines 41-45]. Greenfield doesn't expressively mention said keys being randomly chosen from a common pool. Garay teaches key ring (key subset) including a plurality of individually selectable keys, said keys being randomly chosen from a common pool [col. 5 lines 12-16].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Garay with Greenfield, since one would have been motivated to maintain the security of broadcast to authorized users [Garay, col. 1 lines 11-12].

Greenfield teaches establishing a secure communication link between the node and another nodes [Fig. 3, 5].

Wong teaches:

upon deployment of said plurality of the sensor nodes of the Distributed Sensor Network, at least one sensor node being actuated to discover at least another sensor node sharing said at least one common key to establish a secure communication link between said one and another of said sensor nodes [Fig.1, paragraph 0017 lines 2-5, 0043]; and using said at least one common key for secure communication between said at least one and another sensor nodes over said secure communication link established therebetween [Fig. 2a-3b, paragraph 0043, 0054].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Wong with Greenfield and Garay, since one would have been motivated to provide secure communication between wireless nodes [paragraph 0002].

As per claim 16, it is a system claim corresponds to method claim 1 and is rejected for the same reason set forth in the rejection of claim 1 above.

3. Claims 2, 3, 4, 13, 14, 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Greenfield (US Patent No 6,748,528) in view of Garay et al (US Patent No. 6,839,436) in view of Wong (US Pub. No. 2002/0146127) and in view of Dinsmore et al (US Patent No. 7,043,024).

As per claim 2, the rejection of claim 1 is incorporated and Garay teaches:

for each said sensor node, randomly selecting a distinct set of the keys to form said respective key ring [col. 5 lines 12-16].

Dinsmore teaches:

generating a key space, randomly selecting a pool of keys from said key space, assigning a specific key identifier (e.g. K1, K2,....., K7,.....,K15 etc.) for each key from said pool of keys [Fig. 7].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Dinsmore with Greenfield, Garay and Wong, since one would have been motivated to distribute the key and provide secure group communication in the distributed network [Dinsmore, col. 1 lines 12, 15-17].

As per claim 3, the rejection of claim 2 is incorporated and Dinsmore teaches:

assigning to each said sensor node a specific sensor identifier (e.g. U1, U2, ...etc.) [Fig. 1, col. 11→ table 1].

As per claim 4, the rejection of claim 2 is incorporated and Dinsmore teaches:

loading to said at least one sensor node a specific key identifier of each key on said key ring of said at least one sensor node [col. 11→ table 1, Fig. 6], and broadcasting said key identifiers associated with said at least one sensor node to discover said at least another sensor node [col. 1 lines 17-19, col. 7 lines 60-67, col. 1-3].

As per claim 13, the rejection of claim 1 is incorporated and Dinsmore teaches:

upon expiration of at least one key shared by said at least one and another sensor node, removal of said expired at least one key from said key rings of said at least one and another sensor nodes, and searching for another key common for said at least one and another sensor nodes to establish a new communication link therebetween [col. 12 lines 5-62, Fig. 8A, 9].

As per claim 14, the rejection of claim 2 is incorporated and Dinsmore teaches:

generating a connectivity random graph for said Distributed Sensor Network, and computing the number of the sensor nodes, the number of keys in said pool of keys and the size of each said key ring, sufficient to provide for a connected Distributed Sensor Network [Fig. 13].

As per claim 17, the rejection of claim 16 is incorporated and further claim 17 is a system claim corresponds to method claim 2 and is rejected for the same reason set forth in the rejection of claim 2 above. Further, Dinsmore teaches randomly selecting at least two distinct sets of keys from said pool of keys [col. 7 lines 8-16, Fig. 7].

As per claim 18, the rejection of claim 17 is incorporated and further claim 17 is a system claim corresponds to method claim 4 and is rejected for the same reason set forth in the rejection of claim 4 above.

4. Claims 5 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Greenfield (US Patent No 6,748,528) in view of Garay et al (US Patent No. 6,839,436) in view of Wong (US Pub. No. 2002/0146127) in view of Dinsmore et al (US Patent No. 7,043,024) and in view of Kasahara et al. (U. S. Patent No. 7,080,255).

As per claim 5, the rejection of claim 3 is incorporated and Greenfield teaches plurality of controller nodes (i.e. servers) [Fig. 2].

Dinsmore teaches:

saving said key identifiers of the keys in said respective key ring of each said sensor node along with said sensor identifier of said each sensor node on a trusted controller node from said plurality of controller nodes [col. 11 → table 1, col. 7 lines 58-60].

Kasahara ('255) teaches a plurality of controller nodes associated with said sensor nodes in a predetermined order [Fig. 2].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Kasahara ('255) with Greenfield, Garay, Wong and Dinsmore, since one would have been motivated to provide the cryptographic communication (i.e. secure communication) and high degree of security in the Distributed Sensor Network [Kasahara, col. 3 lines 38, 40].

As per claim 18, the rejection of claim 17 is incorporated and further claim 17 is a system claim corresponds to method claims 4 and 5 and is rejected for the same reason set forth in the rejection of claims 4 and 5 above.

5. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Greenfield (US Patent No 6,748,528) in view of Garay et al (US Patent No. 6,839,436) in view of Wong (US Pub. No. 2002/0146127) in view of Dinsmore et al (US Patent No. 7,043,024) and in view of Briscoe (US Pub. No. 2003/0044017).

As per claim 6, the rejection of claim 4 is incorporated and Dinsmore teaches broadcast the key identifiers [col. 1 lines 17-19].
Briscoe teaches sending the key identifiers (i.e. key index) in a clear text [Fig. 5, paragraph 0064 lines 4-5].
Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Briscoe with Greenfield, Garay, Wong and Dinsmore, since one would have been motivated to provide the cryptographic communication (i.e. secure communication) [Wong, paragraph 0002].

6. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Greenfield (US Patent No 6,748,528) in view of Garay et al (US Patent No. 6,839,436) in view of Wong (US Pub. No. 2002/0146127) in view of Dinsmore et al (US Patent No. 7,043,024) and in view of Akiyama et al (US Pub. No. 2003/0002680).

As per claim 7, the rejection of claim 4 is incorporated and Dinsmore teaches broadcast the key identifiers [col. 1 lines 17-19].

Akiyama teaches transmitting the encrypted key identifiers (i.e. in a hidden pattern) [Fig. 33].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Briscoe with Greenfield, Garay, Wong and Dinsmore, since one would have been motivated to provide the cryptographic communication (i.e. secure communication) [Wong, paragraph 0002].

7. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Greenfield (US Patent No 6,748,528) in view of Garay et al (US Patent No. 6,839,436) in view of Wong (US Pub. No. 2002/0146127) in view of Dinsmore et al (US Patent No. 7,043,024) in view of Kasahara et al. (U. S. Patent No. 7,080,255) and in view of Hardjono (US Patent. No. 6,584,566).

As per claim 8, the rejection of claim 5 is incorporated and Hardjono teaches:

computing a sensor-controller key shared by said each sensor node with said trusted controller, and loading said trusted controller and said each sensor node with said sensor-controller key [Fig. 1].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Hardjono with Greenfield, Garay, Wong, Dinsmore and Kasahara ('255), since one would have been motivated to provide secure multicast communication [Hardjono, col. 1 lines 15-16].

8. Claims 9, 10, 11, 12, 20, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Greenfield (US Patent No 6,748,528) in view of Garay et al (US Patent No. 6,839,436) in view of Wong (US Pub. No. 2002/0146127) in view of Dinsmore et al (US Patent No. 7,043,024) in view of Kasahara et al. (U. S. Patent No. 7,080,255) and in view of Perlman (US Patent No. 5,455,865).

As per claim 9, the rejection of claim 5 is incorporated and Dinsmore teaches:

upon compromising of at least one sensor node, revoking said at least one compromised sensor node by broadcasting from said trusted controller a revocation message (i.e. notification) [col. 12 lines 26-28, Fig. 8A, 9].

Dinsmore teaches revoking the at least one compromised sensor node by notifying from the trusted server [col. 12 lines 26-28]. Dinsmore doesn't expressively mention that message containing a signed list of the key identifiers.

Perlman teaches message containing a signed list of the key identifiers [Fig. 8A].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Hardjono with Greenfield, Garay, Wong, Dinsmore and Kasahara ('255), since one would have been motivated to minimize disruption to message delivery due to malfunctioning nodes in a network [Perlman, col. 2 lines 31-32].

As per claim 10, the rejection of claim 9 is incorporated and Dinsmore teaches the trusted server communicates with the group of N users through N respective unicast communications channels [col. 1 lines 19-21 → i.e. unicasting the signature key to each said sensor node].

As per claim 11, the rejection of claim 10 is incorporated and Perlman teaches receiving the packet and verifying the signature and said signed list of key identifiers [col. 6 lines 35-41].

Dinsmore teaches locating said key identifiers in said key ring of said uncompromised sensor node, and removing keys corresponding to the key identifiers of the compromised keys from said key ring of said uncompromised sensor node [Fig. 9,11 col. 12 → table 2, 3].

As per claim 12, the rejection of claim 9 is incorporated and Dinsmore teaches:

reconfiguring the communication links of the sensor nodes affected by revocation of said compromised sensor node [Fig. 8A, 8B, 10, col. 12 → table 2, 3].

As per claim 20, the rejection of claim 19 is incorporated and further claim 20 is a system claim corresponds to method claim 9 and is rejected for the same reason set forth in the rejection of claim 9 above.

As per claim 21, the rejection of claim 20 is incorporated and further claim 21 is a system claim corresponds to method claim 12 and is rejected for the same reason set forth in the rejection of claim 12 above.

9. Claims 15 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Greenfield (US Patent No 6,748,528) in view of Garay et al (US Patent No. 6,839,436) in view of Wong (US Pub. No. 2002/0146127) and in view of Kasahara et al. (U. S. Patent No. 6,788,788).

As per claim 15, the rejection of claim 1 is incorporated and Kasahara teaches:

assigning a path-key to a selected pair of sensor nodes connected by at least two communication links [Fig. 1, col. 4 lines 1-60, col. 8 lines 45-50].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Kasahara with Greenfield, Garay and Wong, since one would have been motivated to provide the cryptographic communication (i.e. secure communication) [Wong, paragraph 0002].

As per claim 22, the rejection of claim 16 is incorporated and further claim 22 is a system claim corresponds to method claim 15 and is rejected for the same reason set forth in the rejection of claim 15 above.

Response to Amendment

10. Applicant has amended claims 1 and 16 which necessitated new ground of rejection. See rejection above.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Asad et al (US 6539093)---- Key ring organizer for an electronic business using public key infrastructure

Ballard et al (US 2003/0065941) --- Message handling with format translation and key management

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

NBP
6/13/07

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100